CH 8 IDENTITE DE BEZOUT

EX 6 :

1. $2^5 = 32 = 11x3 - 1 \Rightarrow 2^5 \equiv -1(11)$

   $2^5 = 32 = 31x1+1 \Rightarrow 2^5 \equiv 1(31)$

2. **On a $2^5 \equiv -1(11) \Rightarrow (2^5)^{68} \equiv (-1)^{68}(11) \Rightarrow 2^{340} \equiv 1(11)$**

   On a $2^5 \equiv 1(31) \Rightarrow (2^5)^{68} \equiv 1^{68}(31) \Rightarrow 2^{340} \equiv 1(31)$

3. $\left.\begin{array}{l} on\ a\ 2^{340} \equiv 1(31) \Rightarrow 31 divise\ 2^{340}-1 \\ on\ a\ 2^{340} \equiv 1(11) \Rightarrow 11\ divise\ 2^{340}-1 \\ \qquad\qquad et\ comme\ 31 \wedge 11 = 1 \end{array}\right\} \Rightarrow 11 \times 31 = 341 divise 2^{340} - 1$

EX 7 :

1. a^561=1 $\Rightarrow a \wedge (3.11.17) = 1 \Rightarrow \left.\begin{array}{l} a\ n'est\ pas\ un\ multiple\ de\ 3 \\ et\ comme\ 3\ nombre\ premier \end{array}\right\} \Rightarrow a \wedge 3 = 1$

   de même on montre que a^11=1 et a^17=1

2. a/

   $\left.\begin{array}{l} 3\ un\ nombre\ premier \\ a\ n'est\ pas\ un\ multiple\ de\ 3 \end{array}\right\} \overset{fermat}{\Rightarrow} a^{3-1} \equiv 1(3) \Rightarrow a^2 - 1 \equiv 0(3) \Rightarrow 3\ divise\ a^2 - 1$

   b/ de même que a/

   c/ de même que a/

3. a/ On a $a^2 \equiv 1(3) \Rightarrow (a^2)^{280} \equiv 1^{280}(3) \Rightarrow a^{560} \equiv 1(3)$

   On a $a^{10} \equiv 1(11) \Rightarrow (a^{10})^{56} \equiv 1^{56}(11) \Rightarrow a^{560} \equiv 1(11)$

   On a $a^{16} \equiv 1(17) \Rightarrow (a^{16})^{35} \equiv 1^{35}(17) \Rightarrow a^{560} \equiv 1(17)$

   b/

   $\left.\begin{array}{l} a^{560} \equiv 1(17) \Rightarrow 17\ divise\ a^{560} - 1 \\ a^{560} \equiv 1(11) \Rightarrow 11\ divise\ a^{560} - 1 \\ \qquad\qquad et\ comme\ 11 \wedge 17 = 1 \end{array}\right\} \Rightarrow 11 \times 17 divise\ a^{560} - 1 \Rightarrow 187 divise\ a^{560} - 1$

   $\left.\begin{array}{l} on\ a\quad a^{560} \equiv 1(3) \Rightarrow 3\ divise\ a^{560} - 1 \\ \qquad\qquad et\ on\ a\ 187 divise\ a^{560} - 1 \\ \qquad\qquad\qquad 3 \wedge 187 = 1 \end{array}\right\} \Rightarrow 3 \times 187 divise\ a^{560} - 1 \Rightarrow 561\ divise\ a^{560} - 1$